Firewall

Certification Testing Report

A10 Networks, Inc.

Thunder Series Platforms

Tested against these standards

ICSA Labs Firewall Certification Criteria Baseline Module – Version 4.2
ICSA Labs Firewall Certification Criteria Corporate Module – Version 4.2

April 17, 2019

Prepared by ICSA Labs
1000 Bent Creek Blvd., Suite 200
Mechanicsburg, PA 17050
www.icsalabs.com

Table of Contents

Executive Summary

Introduction

The goal of ICSA Labs certification testing is to increase user and enterprise trust in information security products and solutions. For more than 30 years, ICSA Labs, an independent division of Verizon, has been providing credible, independent, 3rd-party security product testing and certification for many of the world's top security product developers and service providers. Enterprises worldwide rely on ICSA Labs to set and apply objective testing and certification criteria measuring product security, compliance and performance.

Summary of Findings

Following rigorous security testing at ICSA Labs, the Thunder 5330(S) satisfied all of the firewall security testing requirements in both the ICSA Labs baseline firewall and ICSA Labs corporate firewall testing standards. As a result, the A10 Networks Thunder Series retained ICSA Labs Firewall Certification having met all of the testing requirements.

Product Overview

The A10 Networks Thunder™ Series from A10 Networks delivers high performance application networking and security solutions. The A10 Networks Thunder™ Series allows for the integration and expansion of system resources to support future feature needs, while offering A10 Networks broadest array of physical, virtual and hybrid form factors.

Scope of Assessment

ICSA Labs tests firewall products against its industry-approved set of testing criteria. Over time, this set of testing criteria became an industry standard. Testing requirements evolved with input from a consortium of firewall vendors, end users, and ICSA Labs. The present iteration of *The Firewall Certification Criteria* is version 4.2.

Continuous Deployment and Spot Checks

Following security testing by ICSA Labs, tested firewalls remain continuously deployed at the labs for the length of the testing contract. When relevant new attacks and vulnerabilities are discovered, all deployed firewall models may be periodically checked to ensure they provide the requisite protection. In the event that any firewall is found susceptible to new attacks or vulnerabilities during a check, ICSA Labs works with the security product vendor to resolve the shortcomings in order for the product to maintain its ICSA Labs Firewall Certification.

Tested Firewall Product Components

Hardware

- Thunder 5330(S)

Software

ICSA Labs began firewall testing with firmware version 4.1.1-P6 Build 62. Testing successfully completed with version 4.1.1-P10 build 69.

Documentation

To satisfy documentation requirements, Thunder Series Platforms provided ICSA Labs with the following documents in order to assist in the installation, configuration, and administration of their firewall product(s):

- *System Configuration and Administration Guide ACOS 4.1.1 -P6*
- *Command Line Interface Reference for CGN ACOS 4.1.1-P6*

Product Family Description

This section lists all ICSA Labs Firewall Certified models from the security vendor's family of related products. While all of the models from the family listed below are certified, the model listed in the Hardware section above is the one or ones tested by ICSA Labs during this test cycle.

Product Family Members

• Thunder 840	• Thunder 930	• Thunder 940	• Thunder 1030S	• Thunder 1040
• Thunder 3030S	• Thunder 3040	• Thunder 3230(S)	• Thunder 3430(S)	• Thunder 4430(S)
• Thunder 4440(S)	• **Thunder 5330(S)**	• Thunder 5430(S)-11	• Thunder 5440(S)	• Thunder 5630(S)
• Thunder 5840(S)	• Thunder 5840-11	• Thunder 6430(S)	• Thunder 6440(S)	• Thunder 6630(S)
• Thunder 7440(S)	• Thunder 7440-11	• Thunder 4435(S) SPE	• Thunder 5435(S) SPE	• Thunder 6435(S) SPE
• Thunder 6635(S) SPE	• Thunder 3030S HVA	• Thunder 3530S HVA	• Thunder 14045	• VThunder ADC

Installation and Configuration

Firewall products can be configured different ways; therefore, ICSA Labs typically makes many configuration related decisions prior to adding a security policy to the firewall. Because ICSA Labs attempts to exploit the product under test, configuration decisions were made in an attempt to make exploitation less likely.

ICSA Labs installed and configured the security vendor's product following the firewall product documentation. Any special configuration changes or deviations from the documentation that were necessary to execute a test or meet a requirement are documented in this section.

- ICSA Labs configured the Thunder 5330(S) in routing mode for both inbound and outbound traffic.

Required Services Security Policy Transition

Expectation

Each phase of firewall testing is performed predominantly while enforcing a particular security policy. Firewall products must be configurable to minimally enforce a security policy such as the one specified in *The Modular Firewall Certification Criteria,* referred to as the Required Services Security Policy or RSSP. The RSSP permits a set of common Internet services inbound and outbound while dropping or denying all other network traffic.

Results

ICSA Labs performed port scans followed by additional scans and other tests to ensure that the security vendor's product was indeed configured according to the RSSP and that no other TCP, UDP, ICMP, or other IP protocol traffic was permitted to or through the firewall in either direction.

After performing the scans mentioned above, ICSA Labs verified that the firewall properly handled all permitted outbound and inbound service requests. ICSA Labs also confirmed that no other traffic traversed the firewall in either direction that would violate the security policy.

ICSA Labs determined through testing that the A10 Networks Thunder Series met all the security policy transition requirements.

Logging

Expectation

Firewalls destined for enterprise and government organizations as well as firewalls provided by managed security services providers need to provide an extensive logging capability. This explains why the breadth and depth of ICSA Labs firewall log testing is so extensive.

ICSA Labs tested the logging functionality provided by the firewall product under test ensuring that all permitted and denied traffic was logged. Analysts in the lab sent traffic both to and (attempted to send traffic) through the product. Other events that must be logged are system startups, time changes, access control rule changes, and administrative login attempts. ICSA Labs typically configures firewall products to send log data for logged events to an external server such as a syslog server. For all logged events ICSA Labs verified that the appropriate, required log data was recorded.

Results

With the A10 Networks Thunder Series of products, logs can be retrieved locally via the web UI, or log events can be sent to an external server such as a syslog server. For this round of certification testing, ICSA Labs configured the Thunder 5330(S) to send log messages to a private syslog server.

The following depicts a failed WebUI login attempt:

```
Apr 10 16:28:37 a10-5330.prop TH5330S a10logd: [SYSTEM]<3> The user, admin,
from the remote host, 172.26.25.214, failed in the web authentication.
```

Initially, the Thunder 5330(S) did not log all traffic necessary to meet the testing criteria. This is described in the "Criteria Violations and Resolutions" section of this report. A10 repaired the shortcomings. Subsequent testing demonstrated that the A10 Networks Thunder Series met all the logging requirements.

Administration

Expectation

Firewall products often have more than a single method by which administration is possible. Whether the product can be administered remotely using vendor provided administration software, from a web browser based interface, via some non-networked connection such as a serial port, or some other means, authentication must be possible before access to administrative functions is granted. ICSA Labs tested not only that authentication mechanisms existed but also that they could not be bypassed and that remote administration traffic was encrypted.

Results

ICSA Labs remotely administered Thunder Series Platforms in the lab from the private network using the available web-based GUI via HTTPS. Attempts to bypass the authentication mechanism for all means of administration were unsuccessful.

ICSA Labs determined through testing that the A10 Networks Thunder Series met all the administration requirements.

Persistence

Expectation

Power outages, electrical storms, and inadvertent power losses should not cause the firewall to lose valuable information such as the remote administration configuration, security policy being enforced, log data, time and date, and authentication data. This section documents the findings of ICSA Labs testing of the firewall product against the persistence requirements.

Results

The Thunder Series Platforms devices continued to maintain their configuration, settings, and data following a forced power outage. Similarly, the products continued to enforce the configured security policy following the outage.

ICSA Labs determined through testing that the A10 Networks Thunder Series met all the persistence requirements.

Documentation

Expectation

ICSA Labs expects firewall documentation to be accurate and applicable to the version tested. The documentation should minimally provide appropriate guidance for installation, configuration and administration.

Results

ICSA Labs determined that the documentation provided adequate and accurate guidance throughout testing for installation and administration.

The documentation provided by A10 Networks met all of the documentation requirements and facilitated the installation and proper configuration of the A10 Networks Thunder Series products.

Functional and Security Testing

Expectation

Once configured to enforce a security policy an ICSA Labs certified firewall must properly permit the services allowed by that policy. In this case, "properly" means that the service functions correctly. The firewall must be capable of preventing well-known, potentially harmful behavior found in some network protocols while at the same time maintaining compliance with applicable network protocol standards in all other ways. In the event of a conflict between these two things, a firewall tested and certified by ICSA Labs must defer to providing increased security. During functional testing ICSA Labs checked to ensure proper protocol behavior for the permitted services.

During security testing, ICSA Labs used commercial, in-house, and freely available testing tools to attack and probe the firewall. ICSA Labs used these tools to attempt to defeat or circumvent the security policy enforced. Additionally, using Denial-of-Service and fragmentation attacks ICSA Labs attempted to overwhelm, bypass or otherwise defeat the enforced security policy.

Since there is overlap between functional and security testing, the results of both phases of testing are presented here.

Results

ICSA Labs determined through testing that the A10 Networks Thunder Series met all the functional and security requirements.

Criteria Violations and Resolutions

Introduction

In the event that ICSA Labs uncovers criteria violations while testing a firewall product, the security vendor must make repairs before testing is successfully completed and certification granted. The section that follows documents all criteria violations discovered during testing.

Results

ICSA Labs found the issues listed below during this test cycle. ICSA Labs reported, and A10 Networks subsequently corrected, these initial shortcomings. The testing product initially:

- Did not properly log failed login attempts to the web-based user interface.

After ICSA Labs confirmed that A10 Networks repaired the above shortcomings ICSA Labs was pleased to once again grant the A10 Networks Thunder Series ICSA Labs firewall certification.

Authority

This report is issued by the authority of the General Manager, ICSA Labs. Tests are performed under normal operating conditions.

Sebastien Mazas, General Manager, ICSA Labs

ICSA Labs

The goal of ICSA Labs is to significantly increase user and enterprise trust in information security products and solutions. For more than 30 years, ICSA Labs, an independent division of Verizon, has been providing credible, independent, 3rd party security product testing and certification for many of the world's top security product developers and service providers. Enterprises worldwide rely on ICSA Labs to set and apply objective testing and certification criteria for measuring product compliance and performance.

www.icsalabs.com

A10 Networks

A10 Networks (NYSE: ATEN) is a provider of intelligent and automated cybersecurity solutions, providing a portfolio of high-performance secure application solutions that enable intelligent automation with machine learning to ensure business-critical applications are secure and always available. Founded in 2004, A10 Networks is based in San Jose, Calif., and serves customers in more than 80 countries with offices worldwide.

www.a10networks.com